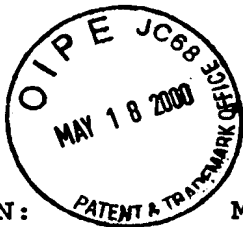


IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



SPECIFICATION

INVENTION: METHOD FOR AUTHENTICATING A SPARE KEY
FOR USING A VEHICLE

INVENTOR: Ruediger BARTZ
Citizenship: German
Post Office Address/ Connollystr. 15 K
D-80809 Muenchen
Residence: Germany

ATTORNEYS: EVENSON, McKEOWN, EDWARDS & LENAHAAN, P.L.L.C.
Suite 700
1200 G Street, N.W.
Washington, D.C. 20005
Telephone No.: (202) 628-8800
Facsimile No.: (202) 628-8844

METHOD FOR AUTHENTICATING A SPARE KEY FOR USING A VEHICLE

BACKGROUND AND SUMMARY OF THE INVENTION

This application claims the priority of German Application No. 199 01 277.6, filed January 15, 1999, the disclosure of which is expressly incorporated by reference herein.

The invention relates to a method for authenticating a spare vehicle key for use with a vehicle.

A method of this type is known from European Patent document EP 0 788 946 A. In this reference, with the aid of a separate programming unit located outside the vehicle, data specific to a part of the vehicle are retrieved from a central station, transmitted from the central station to the programming unit, and transferred from the latter to the vehicle. The data are then decoded in the vehicle. Although double coding is used some of the time, problems may arise with the known method if the separate programming unit is misused.

Overall, it should be noted that the general trend to increase protection against theft and break-ins runs counter to the customer service requirement of being able to open and move a vehicle when the original key is not present, for example if the original key has been lost or inadvertently locked inside the

vehicle. The problem becomes even more acute when burglar-proof glass is used.

The goal of the invention is therefore to create a method of the type referred to above that is easy to perform and use, as well as being protected against misuse.

The invention achieves this goal by providing a method for authenticating a spare key to be used in a vehicle in the absence of the regular key. The spare key is provided with an identification number that is transmitted to, and checked by, a central station. The spare key is authenticated by an authorization signal sent by the central station to the vehicle.

The essential point of the invention is authentication of the spare key by the central station. Since the identification number of the spare key is transmitted to, and checked by, the central station, obvious misuse of a spare key that has been lost for example, as soon as this fact is communicated to the central station, is recognized and transmission of the authorization signal from the central station to the vehicle is prevented.

Advantageous embodiments of the invention are explained in greater detail in the description of the method based on the figures.

Advantageously, at least some of the data transmissions, such as from the spare key to the central station or from the central station to the vehicle are encoded. In particular, the data transmissions are encoded with a random number. In a particular preferred embodiment, bidirectional data traffic occurs wherein the data transmission takes place in one direction followed by transmission of a confirmation signal in an opposite direction. Further advantageously, the bidirectional data traffic in the one direction takes place based on a public key and the decoding at the central station takes place based on private key.

In a particularly advantageous embodiment, the transmission of the spare key identification number to the central station is performed by the vehicle itself, to which the spare key identification number was previously transmitted.

Also advantageously, data transmission can take place via telephony.

In another advantageous embodiment, before the actual data transmission occurs, a receiver is activated by the spare key.

Other objects, advantages and novel features of the present invention will become apparent from the following detailed

description of the invention when considered in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The single figure is a block diagram showing the operative switchpoints and transmission paths of the method according to the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

The method described here provides the possibility of opening and operating a vehicle 5 with the aid of a universally applicable spare key without impairing the effectiveness of theft protection. When the spare key is authenticated by a central station 6 using the car phone and a central database, a temporary authorization at least to open the vehicle using the spare key is granted.

The universally applicable spare key 10 is called a VK key below. Other operating points in the context of the method are the central database 12 (called VK database), a car phone present in the vehicle 14, a base interface telephone 16 (called BIT interface), and a cellular telephone of a customer service representative who brings the spare key into use 18. It is also important to use preferably asynchronous algorithms for telephone calls. This makes it unnecessary to ensure that telephone calls

are not being tapped. An "asynchronous algorithm" is understood to be an encoding method that in one direction operates with a public encoding algorithm (public key) and for decoding operates with a secret encoding algorithm (secret "private" key).

5 The evaluation of the signals arriving at the vehicle is preferably effected by the CAS (car access system) control unit 22 that has a ring memory in which the successful VK key authentications are stored and any attempts at manipulation are stored in an attack memory.

10 The entire process of opening the vehicle with the spare key takes place in five steps, I through V as described below and indicated in the Figure.

I) By pressing a command key on the VK key, the spare key 10 generates a random number PIN which is decoded and, together with an individual recognition of the spare key VK_KEY_ID is transmitted to the vehicle with a non-secret (= public) code. The radio receiver 28 of the vehicle receives this radio-transmitted encoded signal $Krypt_{fl}(VK_KEY_ID, PIN)$ and the random number PIN and sends it to the CAS 22, where the recognition of the spare key VK-KEY-ID is decoded based on recognition of the random number PIN.

15

20

II) The service technician transmits the following data, preferably using his cellular telephone 18, to the VK database 6:

random number PIN, and the telephone number and chassis number of the vehicle. With telephone transmission, coding is unnecessary.

Using the chassis number, the VK database 6 finds the corresponding public key of the vehicle (P-CODE-FZG) and uses it to encode the random number PIN.

III) The car phone 14 is dialed from the VK database and the encoded random number PIN is transmitted, received by the car phone, and forwarded to the CAS control unit 22. The CAS has a secret decoding algorithm secret key (S-CODE-Vehicle) which enables it to regenerate the random number PIN without actually knowing this PIN. The PIN is then compared with the PIN received in step I.

IV) If the two PINs are identical, the CAS 22 generates its own random number RAND. RAND and the recognition VK_KEY-ID of the spare key transmitted thereto in step I are each encoded with a public key P-CODE-VK and transmitted to the VK database 6 via the car phone 14. At the VK database, using the secret key S-CODE-VK, the random number RAND and the VK key identifier VK-KEY-ID are regenerated and checked

to see whether the VK key identifier VK_KEY-ID is assigned to a valid spare key. Separate knowledge of the random number RAND is not necessary for this regeneration.

V) If the VK key identifier is valid, the random number RAND in response is encoded with a public key P-CODE-Vehicle and transmitted to the CAS 22 in the vehicle 5. The vehicle is able to regenerate the random number RAND with its secret key S-CODE-Vehicle and compare it with the key in its memory. If the two are identical, this is interpreted as validation of the spare key VK_Key and the commands issued with the VK_Key are executed.

It should be understood that the structure and operation of the various components used in the system to perform the method according to the present invention are well known by those of skill in the art. As such, they have not been described in detail here, but rather only the inventive method acts for authenticating the spare vehicle key to be used in the vehicle in the absence of the regular key.

The foregoing disclosure has been set forth merely to illustrate the invention and is not intended to be limiting. Since modifications of the disclosed embodiments incorporating the spirit and substance of the invention may occur to persons skilled in the art, the invention should be construed to include

everything within the scope of the appended claims and equivalents thereof.